Solutions to Re-exam in MM7033, 2024-01-30, 8:00–13:00

1. (a) The polynomial $f(x) = x^4 - 1 = (x^2+1)(x+1)(x-1)$ has two roots in $\mathbb{R}$, $x = 1$ and $x = -1$. Thus $\mathcal{Z}(f) = \{1, -1\}$. The polynomials vanishing at both $x = 1$ and $x = -1$ are those divisible by $x^2 - 1$ so $\mathcal{I}\big(\mathcal{Z}(f)\big) = (x^2 - 1)$. Note that $\mathcal{I}\big(\mathcal{Z}(f)\big)$ is not the radical of (f), which equals (f) — the Nullstellensatz does not apply since $\mathbb{R}$ is not algebraically closed.

   (b) The subset $\mathbb{N}$ is infinite. A non-zero polynomial $p(x)$ has at most as many roots as its degree. We thus conclude that $\mathcal{I}(\mathbb{N}) = (0)$. It follows that $\mathcal{Z}\big(\mathcal{I}(\mathbb{N})\big) = \mathbb{A}^1$.

2. (a) Suppose $[E : F] = 2$. Then for every $\alpha \in E$, the elements $1, \alpha, \alpha^2$ are linearly dependent over F. It follows that the minimal polynomial of α in $F[x]$ has degree at most 2, and since it has a root in E it splits completely over E.

   (b) The extension $\mathbb{Q}(\sqrt[3]{2})$ of $\mathbb{Q}$. The polynomial $p(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$ and $\sqrt[3]{2}$ is a root of $p(x)$ in $\mathbb{Q}(\sqrt[3]{2})$. It follows that $p(x)$ is the minimal polynomial of $\sqrt[3]{2}$. But it does not split completely over $\mathbb{Q}(\sqrt[3]{2})$ since the other roots of this polynomial are complex.

   (c) Let F be a finite field and L/F an algebraic extension. Let $\alpha \in L$, and $p(x) \in F[x]$ the minimal polynomial of α. Let $F(\alpha) \subset L$ be the subfield generated by F and α. Then $F(\alpha)$ is a finite extension of F, and therefore is itself a finite field. It is enough to prove that $p(x)$ splits completely in $F(\alpha)$. This means that we may assume that L itself is a finite field.

   Let p be the characteristic of F. We may assume that F has p^k elements and L has p^n elements, for some $k < n$. The elements of L are all roots of the polynomial $x^{p^n} - x$, which splits completely in L. It follows that the minimal polynomial of α over F is a factor of $x^{p^n} - x$, and therefore it splits completely in L.

3. Suppose first that for every finitely generated M, the homomorphism $A \otimes M \to B \otimes M$ is injective. Taking $M = \mathbb{Z}/n$, we obtain that the homomorphism $\varphi\colon A \otimes \mathbb{Z}/n \to B \otimes \mathbb{Z}/n$ is injective. We saw in class that $B \otimes \mathbb{Z}/n \cong B/nB$, where nB is the image of the homomorphism $B \xrightarrow{\cdot n} B$, i.e., the group of all elements of B that are divisible by n. We can thus identify the homomorphism φ with the homomorphism $A/nA \to B/nB$, taking $a + nA$ to $a + nB$. That this homomorphism is injective means that an element of A is divisible by n if and only if its image in B is divisible by n. This is equivalent to saying that A is a pure subgroup of B.

   Now suppose that A is a pure subgroup of B. By classification of finitely generated abelian groups and the fact that $A \otimes (M \oplus M') \cong (A \otimes M) \oplus (A \otimes M')$, it is enough to prove that the homomorphism $A \otimes M \to B \otimes M$ is injective when $M = \mathbb{Z}$ or $M = \mathbb{Z}/n$. The case $M = \mathbb{Z}$ is obvious, and the case $M = \mathbb{Z}/n$ is proved by reversing the logic of the first part. Indeed, since $A \subset B$ is pure, an element $a \in A$ is divisible by n if and only if its image in B is divisible by n. Thus $A/nA \to B/nB$ is injective.

4. (a) R/P is an integral domain such that $x^2 = x$ for every $x \in R/P$. Indeed, this follows from $x^2 = x$ for every $x \in R$ since $R \to R/P$ is surjective. Since R/P is a domain, $x^2 = x$ implies that either $x = 0$ or $x = 1$. Thus, R/P has exactly two elements and is thus isomorphic to the finite field with two elements $\mathbb{F}_2$. Since R/P is a field, P is maximal.

   (b) R_P is a local ring such that $x^2 = x$ since $(r/f)^2 = r^2/f^2 = r/f$ for all $r \in R$ and $f \notin P$. Since $(x, x-1) = (1)$, the elements x and $x - 1$ cannot both be in the unique maximal ideal PR_P. Since $R_P \smallsetminus PR_P = (R_P)^\times$, it follows that either x or $x - 1$ is a unit. From $x(x-1) = 0$ it follows that either $x = 0$ or $x = 1$ and again that $R_P = \mathbb{F}_2$.

5. Since M is finite, it is necessarily a finitely generated torsion module. Thus, since R is a PID, by the structure theorem of finitely generated modules over PIDs, we have that

$$M = R/(p_1^{e_1}) \oplus R/(p_2^{e_2}) \oplus \cdots \oplus R/(p_n^{e_n})$$

for some positive integer n, some irreducible polynomials $p_i \in R = \mathbb{F}_2[x]$ and some positive integers e_i. The factors are unique up to permutation. The irreducible polynomials p_i are unique up to units, hence unique: the units in $\mathbb{F}_2[x]$ are $\mathbb{F}_2^\times = \{1\}$.

Note that x^2+x+1 is irreducible. If $p \neq x^2+x+1$, then $(p^e, x^2+x+1) = (1)$ so x^2+x+1 is invertible in $R/(p^e)$ and so $R/(p^e) = (R/(p^e))_{x^2+x+1}$. If $p = x^2+x+1$, then $(R/(p^e))_{x^2+x+1} = 0$ since $(x^2+x+1)^e \cdot 1 = 0$ in $(R/(p^e))_{x^2+x+1}$. We thus have that

$$M = R/((x^2+x+1)^{e_1}) \oplus \cdots \oplus R/((x^2+x+1)^{e_r}) \oplus R/(x^2) \oplus R/((x-1)^3).$$

Since the dimension of M as a vector space is 9, it follows that $e_1 + \cdots + e_r = 2$ which gives exactly two possible modules up to isomorphism:

$$\begin{aligned} M &= R/((x^2+x+1)^2) \oplus R/(x^2) \oplus R/((x-1)^3) \\ M &= R/(x^2+x+1) \oplus R/(x^2+x+1) \oplus R/(x^2) \oplus R/((x-1)^3). \end{aligned}$$

6. (a) The ideals of $R = \mathbb{Q}[x]/(x^3-1)$ are in bijection with ideals of $\mathbb{Q}[x]$ that contains (x^3-1). This gives the trivial ideal (0), which is free of rank 0 hence projective, the improper ideal $(1) = R$, which is free of rank 1 hence projective, and the two ideals $(x-1)$ and (x^2+x+1). To see that the latter two ideals are projective, consider the sequence

$$0 \longrightarrow (x-1) \longrightarrow R \longrightarrow R/(x-1) \longrightarrow 0. \tag{1}$$

The surjection $\pi\colon R \to R/(x-1)$ has a splitting $s\colon R/(x-1) \to R$ given by sending 1 to $r := \frac{1}{3}(x^2+x+1)$. Indeed $(x-1)r = 0$ so s is well-defined and $\pi(r) = 1$ so s is a section. Thus, $R = (x-1) \oplus R/(x-1)$. Since (x^2+x+1) is principal and annihilated by $(x-1)$, we also see that $R/(x-1) \cong (x^2+x+1)$. Thus both $(x-1)$ and (x^2+x+1) are direct summands of R, hence projective.

(b) We saw in (a) that the sequence (1) was split. It follows that the inclusion $(x-1) \to R$ has a retraction. If we choose the isomorphism $(x^2+x+1) \to R/(x-1)$ which takes x^2+x+1 to 3 then the section s that we constructed in (a) becomes the inclusion $(x^2+x+1) \to R$ which thus also has a retraction. This means that for every ideal J (there are four of these), the inclusion $J \subseteq R$ has a retraction $r\colon R \to J$ (or equivalently the quotient $R \to R/J$ has a section $R/J \to R$) so that

$$0 \longrightarrow J \longrightarrow R \longrightarrow R/J \longrightarrow 0$$

is split exact. It follows that the sequence

$$0 \longrightarrow \mathrm{Hom}_R(R/J, M) \longrightarrow \mathrm{Hom}_R(R, M) \longrightarrow \mathrm{Hom}_R(J, M) \longrightarrow 0$$

is split exact for all R-modules M. In particular $\mathrm{Hom}_R(R, M) \to \mathrm{Hom}_R(J, M)$ is surjective so M is injective by Baer's criterion.